# DM 08
## à rendre le lundi 1er décembre

**Conseils.** Indiquer en début de copie la formule choisie.

- Bases : exercice 1 (1h)
- Intermédiaire : exercices 1 et 2 (Total : 2h)
- Avancé : tout (Total : 3h)

**Exercice 1.** *Théorème de Wilson*. Soit $p$ un nombre premier différent de 2.

1. Montrer que $(p-1)^2 \equiv 1[p]$.
2. Montrer que $x^2 \equiv 1[p]$ si, et seulement si $x \equiv 1[p]$ ou $x \equiv -1[p]$.
3. Soit $n$ dans $\{1, 2, \dots, p-1\}$ Montrer qu'il existe un unique entier $m$ dans $\{1, 2, \dots, p-1\}$ tel que $mn \equiv 1[p]$. Quand a-t-on $m = n$ ?
4. Démontrer que $(p-1)! \equiv p-1[p]$.
5. Déduire de ce qui précède une preuve du théorème de Wilson : pour tout entier naturel $q$, $q$ est premier si, et seulement si $(q-1)! \equiv q-1[q]$.

**Exercice 2.** On note, pour tout entier naturel $n$, $\mathcal{P}(n) = \{k \in [\![0, n-1]\!],\ k \wedge n = 1\}$ l'ensemble des entiers strictement inférieurs à $n$ et premiers avec $n$. On note $\varphi(n)$ le nombre d'éléments de $\mathcal{P}(n)$.

1. Si $p$ est premier et $\alpha$ est dans $\mathbb{N}$, montrer que $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.
2. Soient $m$ et $n$ deux entiers premiers entre eux. Soit $\theta$ l'application qui à $k \in \mathcal{P}(mn)$ associe le couple $(r, s)$ où $r$ est le reste de la division euclidienne de $k$ par $m$ et $s$ est le reste de la division euclidienne de $k$ par $n$.
   (a) Montrer que $\theta$ est à valeurs dans $\mathcal{P}(m) \times \mathcal{P}(n)$.
   (b) Soient $(r, s)$ dans $\mathcal{P}(m) \times \mathcal{P}(n)$. Montrer que le système de congruences
   $$\begin{cases} k \equiv r[m] \\ k \equiv s[n] \end{cases}$$
   d'inconnue $k \in [\![1, mn]\!]$, admet une unique solution, et que cette solution est dans $\mathcal{P}(mn)$.
   (c) Conclure que si $n$ et $m$ sont premiers entre eux, $\varphi(mn) = \varphi(m)\varphi(n)$.
3. Si $n$ est un entier naturel et $\prod_{i=1}^{r} p_i^{\alpha_i}$ sa décomposition en facteurs premiers, que vaut $\varphi(n)$ ?

**Exercice 3.** *Lemme LTE (« Lifting the exponent »)*. Si $n$ est un entier négatif, on définit $v_p(n)$ comme étant $v_p(|n|)$. Ainsi, $v_3(-45) = 2$. Le but de ce problème est de démontrer les jolis Lemmes LTE.

- **Lemme LTE.** Soit $p$ un nombre premier **différent de** 2. Soient $a, b$ des nombres entiers relatifs et un entier $n \geqslant 1$. On suppose que $p$ divise $a-b$ mais que $p$ ne divise ni $a$, ni $b$. Alors :
  $$v_p\left(a^n - b^n\right) = v_p(a-b) + v_p(n).$$
- **Second Lemme LTE.** Soit $p$ un nombre premier **différent de** 2. Soient $a, b$ des nombres entiers relatifs et un entier $n \geqslant 1$ **impair**. On suppose que $p$ divise $a+b$ mais que $p$ ne divise ni $a$ ni $b$. Alors :
  $$v_p\left(a^n + b^n\right) = v_p(a+b) + v_p(n).$$

Fixons alors $p$ un nombre premier impair, $a, b$ des nombres entiers relatifs et un entier $n \geqslant 1$ tels que $p$ divise $a - b$ mais que $p$ ne divise ni $a$, ni $b$.

## A. Cas où $n \wedge p = 1$

**Dans cette partie, on suppose que $n$ et $p$ sont premiers entre eux.**

**1.** Démontrer que $a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + b^{n-1} \equiv na^{n-1}[p]$, puis en déduire que $p$ ne divise pas $a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + b^{n-1}$.

**2.** En déduire que $v_p(a^n - b^n) = v_p(a - b)$.

## B. Cas général

On note $k$ l'entier tel que $b = a + kp$.

**3.** Démontrer que pour tout $i$ entre 0 et $p - 1$,

$$b^i a^{p-1-i} \equiv a^{p-1} + ikpa^{p-2}[p^2]$$

**4.** Par la même méthode qu'en 2., en déduire que $v_p(a^p - b^p) = v_p(a - b) + 1$.

**5.** Conclure que pour tout $\alpha$ dans $\mathbb{N}$, $v_p(a^{p^\alpha} - b^{p^\alpha}) = v_p(a - b) + \alpha$.

**6.** Démontrer les deux Lemmes LTE.

## C. Applications

**7.** On remarque que $2023 = 7 \times 17^2$. Calculer $v_7(60^{2023} - 11^{2023})$.

**8.** Trouver tous les nombres premiers $p$ tels que $(p-1)^p + 1$ soit une puissance de $p$.

**9.** Soient $a, n$ deux entiers strictement positifs et $p$ un nombre premier impair tel que $a^p \equiv 1[p^n]$. Montrer que $a \equiv 1[p^{n-1}]$.